

АСПЕКТИ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

гл.ас. д-р Константин Пудин

Катедра „Национална и регионална сигурност“, УНСС
kopud@unwe.acad.bg

Резюме: Живеем във време, в което информацията и информационните технологии са придобили огромно значение както в деловия живот, така и в личния живот на милиарди хора на планетата. При тази информационно доминирана среда на преден план излизат въпросите на сигурността на информацията на личностно, групово/организационно и държавно ниво. Настоящият доклад е посветен на някои от аспектите на информационната сигурност, касаещи личността, организацията и държавата.

Ключови думи: сигурност, равнища на сигурност, информационна сигурност, тайна.

Въведение.

Ако се замислим, можем ли да си представим ежедневието без ползването на всякакъв вид комуникационни и информационни технологии, ще установим, че това е абсолютно невъзможно. Очевиден факт. Не случайно съвременното общество е наречено информационно. Информацията е всепроникваща и от най-различно естество. Тя буквално ни залива ежеминутно от най-различни източници – радио, телевизия, вестници, мобилни телефони, пейджъри и разбира се най-вече интернет. Наред с това сме свидетели как ежегодно в живота ни навлизат нови все „по-интелигентни“ машинки, които трябва да го направят по-удобен, служейки за по-бързото и по-сигурно пренасяне, съхраняване, създаване на...информация.

При тези обществени условия ясно се откроява нарастващата роля на информацията като ресурс за развитие на отделната личност и на всички образования над нея – група, организация, държава и т.н. Ресурс, който трябва да бъде ценен и защитаван. Успоредно с това се забелязва бум в развитието на информационните и комуникационни технологии. Очертава се тенденцията, че който иска да бъде конкурентоспособен, който иска да успее и да бъде на върха задължително трябва да е в крак с този непрекъснат процес на обновяване и усъвършенстване.

Настоящият доклад разглежда въпроса за информацията, от гледна точка на информационната сигурност на отделни обществени субекти и по-конкретно – сигурността на личностно, групово и държавно равнище (без регионално и световно). Изложението е структурирано в две части. В първа част накратко се представят

различните субекти на сигурността, изяснява се понятието информация. Втората част на доклада е посветена на мерките, които се взимат за обезпечаване на информационната сигурността на тези субекти.

За субектите на сигурността, същността на информацията и информационната сигурност.

Субекти на сигурността са всички обществени субекти, които се нуждаят от такива условия на средата – икономически, политически, социални, екологични, информационни и др., които се характеризират с отсъствие на заплахи или опасности за тяхното съществуване и развитие. Това от своя страна е гаранция за системно и последователно реализиране на разнородните им интереси.

Ако се изхожда от теорията за равнищата на сигурност/схема на петте нива на сигурност, като субекти на сигурността могат да бъдат обособени отделната личност, различните неформални и формални групи, в т.ч. семейство, колективи в стопански и нестопански организации и т.н., държавата, даден регион или световната система от междудържавни отношения (б.а. – Схемата на Петте нива на сигурността е предложена от Н. Слатински през 1999 г. През 2008 г. Д. Йончев публикува книгата „Равнища на сигурност“, в която се позовава на предложената Схема и развива своите възгледи по въпроса.[3, 6]).

В най-широк план **сигурността на отделната личност** се свързва със създаване на условия за спазване и активно упражняване на основните ѝ човешки и граждански права, които са регламентирани в редица международни и национални документи.

Груповата сигурност предполага наличие на среда, благоприятстваща създаването, съществуването, развитието и постигането на целите на различни обединения от хора.

Държавната сигурност е по-сложна, защото обхваща много на брой субекти на сигурността от по-ниските нива.

Държавата е форма на политическа организация на обществото, притежаваща абсолютна власт. Призвана е да гарантира „общото благо“, благо на своите граждани.[2] Това може да означава много неща – осигуряване на траен мирен ред, закрила на справедливостта в общуването между хората, защита от външна агресия, запазване на териториалната цялост и националното и държавно единство и др.

Държавна сигурност има, когато не се наблюдават заплахи или опасности за установената обществена система, функционирането на държавните институции, спазени са принципите за разделение на властите и върховенство на закона. Всичко това от своя страна допринася за генериране на сигурност на личностно и групово равнище.

Както бе отбелязано в началото, субектите на сигурността съществуват и си взаимодействат в изключително динамична информационна среда. Тя е външна за всеки един от тях, но и вътрешна (особено на равнище група, организация и на по-високи равнища). Именно поради това информационният аспект на сигурността на различните субекти се явява изключително актуален, сложен и важен.

Разглеждайки въпроса за сигурността на информацията, на преден план излиза необходимостта от дефиниране на самото понятие. Въпреки че то е толкова разпространено като смисъл и употреба, че за някой това би изглеждало излишно.

Информацията може да бъде дефинирана по различни начини. В най-тесен и конкретен смисъл тя представлява съвкупност от символи, притежаващи определен смисъл.

В широк контекст информацията може да бъде представена като знание, идеи и т.н.

Значимостта или важността е основно качество на информацията. Това, което я прави важна е нейният смисъл и значение за отделния човек, за организацията или държавата. Значимостта се свързва с реализирането на интересите на тези субекти.

Информационната сигурност има различни измерения, като по своята същност тя се свежда до гарантиране тайната на информацията, нейната цялостност и наличност, а също надеждност на средствата за комуникация.

Според дефиницията на същото понятие, дадена в стандарт ISO17799 от 2004, става дума за процес на защита на информацията и информационните активи от множество заплахи, така че да се гарантира непрекъснатост на бизнес процеса, минимизиране на щетите, максимизиране на възвръщаемостта на инвестициите и възможностите на бизнеса чрез опазване тайната, целостта и наличността на информацията.

За тайната и сигурността на информацията на отделните субекти на сигурността.

За по-доброто разбиране на проблематиката за сигурността на информацията на трите равнища – личностно, групово/организационно и държавно трябва да бъдат направени някои пояснения.

На първо място се налага изясняване на понятието „тайна“. Казано най-просто, по своята същност това е информация, която се отличава от останалата информация най-малко по две характеристики – своята значимост и ограничения кръг от лица, които имат достъп до нея. Във всички случаи второто се явява следствие от първото.

Важността на информацията може да бъде измерена чрез ползите или вредите, които тя ще принесе на субекта, който я създава, съхранява и/или за когато се отнася. В икономическия живот най-често тези положителни и отрицателни ефекти могат да бъдат измерени в пари. Но не са малко случаите, когато става дума за нанасянето и на чисто морални щети.

Характерно за информацията, представляваща тайна, е, че колкото по-високо е равнището на сигурност, толкова по-голям е броят на лицата, чиито интереси тя засяга и по-сложни от институционална гледна точка стават мерките за нейното опазване.

Условно можем да обособим тайната в няколко групи. В зависимост от естеството на информацията говорим за икономическа тайна, финансова тайна, военна тайна, производствена тайна и т.н. Ако се изхожда от субекта, който притежава информацията и за който тя се отнася, налице е лична тайна, организационна (корпоративна) тайна, държавна тайна.

Не е изключено тайната да има двойствен характер. Например държавната тайна да бъде едновременно икономическа, военна и т.н. От своя страна организационната тайна може да бъде финансова или пък производствена.

Личната тайна е информация, която касае частния живот на една или няколко личности. Тя засяга вътрешния свят и най-интимните страни от живота на човека.

Организационната тайна е важна информация за функционирането на организацията. Ако става дума за бизнес единица, тогава тя може да бъде наречена фирмена или корпоративна тайна. Такава информация са сведения за размера на продажбите, за технологията на производство, за бъдещи инвестиционни проекти и т.н. Опазването на фирмената тайна е предпоставка за постигане целите на фирмата и защита на нейните интереси. Ето защо това е съществена страна от системата за гарантиране на фирмената сигурност.

Изхождайки от потребителите на информацията, представляваща организационна тайна, които в случая се явяват служители в компания или учреждение, тя може да бъде наречена – служебна тайна.

Държавната тайна е информация от изключителна важност за развитието на обществото и държавата, респективно за реализирането на националните интереси. Поради това нейното опазване е свързано с гарантиране на националната сигурност.

Очевидно е, че след като една информация е толкова важна, то ще бъде ограничен и броят на лицата, които ще имат достъп до нея. Това е, както бе посочено, втората характеристика на информацията, представляваща тайна.

Колкото по-малко субекти и техните интереси касае една информация, представляваща тайна, толкова по-лесно би било нейното опазване. По-малък ще бъде и кръгът от хора, които ще имат достъп до нея. При равни други условия, такъв е случая с личната тайна. Нещата се усложняват, когато става дума за организационна тайна. Разширява се и кръгът на хората, за които ще бъде известна тя и които ще работят с нея.

Още по-сложно е когато става дума за защита на информация, представляваща държавна тайна. Тя е от значение за нормалното протичане на обществените процеси и функционирането на държавата и предполага ограничаването на достъпа до нея само за определена категория/и лица. За целта се разработват специални правни норми, които регламентират начините на нейното създаване, съхраняване, размножаване, ползване и унищожаване, а също изискванията към лицата, имащи достъп до нея. Въвежда се категорията „класифицирана информация”.

Понятието „класифицирана информация” може да бъде разглеждано в широк и тесен, конкретен контекст. Най-свободно при разговори то може да бъде използвано като синоним на всякакъв вид важна, чувствителна информация, в т.ч. и на организационно ниво, достъп до която трябва да имат ограничен кръг лица. Макар логически правилно, това не би било вярно от чисто правна и терминологична гледна точка.

Когато се търси прецизност и конкретност при употреба на понятието, тогава под класифицирана информация трябва да се има предвид, че класификацията е средство за защита на информация и данни, представляващи преди всичко държавна тайна или тайна, свързана с националните интереси.

Срещу „класифицирана информация” в Wikipedia е записано следното „чувствителна информация, достъпът до която е ограничен със закон или друг нормативен акт. За работа с класифицирани документи и класифицирани данни се изисква официално разрешително за достъп. Процесът за получаване на разрешително изисква проучване на миналото на лицата. Тъй като съществуват различни нива на чувствителност на информацията (б.а. – изискващи различни нива на класификация), то и проучванията, които се провеждат са различни”. [7]

Въпросът със защитата на класифицираната информация в България получава своята правна регламентация през 2002 г., когато от XXXIX-то Народно събрание е приет Закона за защита на класифицираната информация (ЗЗКИ). С него се уреждат обществените отношения, свързани със създаването, обработването и съхраняването на класифицирана информация, както и условията и реда за

предоставяне на достъп до нея. Още в края на същата година Министерският съвет приема и Правилник за прилагане на Закона за защита на класифицираната информация (ППЗЗКИ).

Заклучение

В заключение, като се има предвид изложението на доклада, могат да бъдат направени някои обобщения.

Очевиден е фактът, че ролята на информацията и информационните технологии в личния, деловия и държавния живот ще нараства.

Информацията става все по-значим ресурс, който трябва да се притежава, ползва по най-добрия начин и защитава, като целта е реализиране в най-голяма степен на интересите на различни обществени субекти.

Субектите на различните равнища на сигурност предприемат различни мерки за осигуряване на информационния аспект на сигурността. Колкото по-високо е нивото на сигурност, толкова по-сложен от организационно-правна гледна точка стои въпросът за работата с информация, категоризирана като „тайна”.

Гарантирането на тайната, целостта и наличността на информацията, а от тук и непрекъснатостта на процесите на различните нива, е свързано с отделянето на значителни финансови ресурси и време.

Може да бъде изказана и хипотезата, че с нарастване значението на информационните и комуникационни технологии и стремителното им навлизане в ежедневието, ще се засили зависимостта на човека от тях до степен, при която трудно ще бъде да се определи, кой на кого служи. Дори и днес можем да посочим множество примери за това как компютърът не е само част от работното ежедневие, но се е превърнал в смисъл и начин на живот. Разбира се това е само хипотеза, която подлежи на опровержение или доказване.

Използвана литература:

1. Закон за защита на класифицираната информация, Обн. ДВ. бр.45 от 30 Април 2002г., попр. ДВ. бр.5 от 17 Януари 2003г., изм. ДВ. бр.31 от 4 Април 2003г., изм. ДВ. бр.52 от 18 Юни 2004г., доп. ДВ. бр.55 от 25 Юни 2004г., доп. ДВ. бр.89 от 12 Октомври 2004г., изм. ДВ. бр.17 от 24 Февруари 2006г., изм. ДВ. бр.82 от 10 Октомври 2006г., изм. ДВ. бр.46 от 12 Юни 2007г., изм. ДВ. бр.57 от 13 Юли 2007г., изм. ДВ. бр.95 от 20 Ноември 2007г., изм. ДВ. бр.109 от 20 Декември 2007г., изм. ДВ.

бр.36 от 4 Април 2008г., изм. ДВ. бр.66 от 25 Юли 2008г., изм. ДВ. бр.69 от 5 Август 2008г., изм. ДВ. бр.109 от 23 Декември 2008г., изм. ДВ. бр.35 от 12 Май 2009г., изм. ДВ. бр.42 от 5 Юни 2009г., изм. ДВ. бр.82 от 16 Октомври 2009г., изм. ДВ. бр.93 от 24 Ноември 2009г., изм. ДВ. бр.16 от 26 Февруари 2010г., изм. ДВ. бр.88 от 9 Ноември 2010г., изм. ДВ. бр.23 от 22 Март 2011г., изм. ДВ. бр.48 от 24 Юни 2011г.

2. Друмева, Е., *Конституционно право*, СИЕЛА, С. 2008 г.

3. Йончев, Д., *Равнища на сигурност*, НБУ, С. 2008 г.

4. Павлов, Г., *Защита на информацията*, УИ „Стопанство”, С. 2010 г.

5. Павлов, Г., К. Пудин, *„Информационна сигурност в организацията”*, УИ „Стопанство”, С. 2011 г.

6. Слатински, Н., *„Петте нива на сигурността”*, Военно издателство, С. 2010 г.

7. Wikipedia, http://en.wikipedia.org/wiki/Classified_information, сайтът е посетен на 01.11.2011 г.